

## CLAIMS:

- 1           1.     A computer program product for implementing electronic commerce  
2 systems, each electronic commerce system comprising a web site being accessible by  
3 one or more users and comprising a set of on-line stores and a set of organizations,  
4 each of the said on-line stores being associated with one of the set of organizations,  
5 the computer program product comprising a computer usable medium having  
6 computer readable program code means embodied in said medium, and comprising:  
7           computer readable program code means for representing the users, each user  
8                   being associated with a unique identity in the system;  
9           computer readable program code means for associating a user identity with  
10                   one of a set of access roles for a security domain, the access role  
11                   defining access privileges for the user corresponding to the user  
12                   identity, the security domain comprising a subset of the set of  
13                   organizations and the on-line stores associated with the organizations  
14                   in the subset; and  
15           computer readable program code means for granting or denying access to a  
16                   user attempting to access a portion of the web site by determining the  
17                   user identity for the user and determining the access role associated  
18                   with the user identity for the security domain corresponding to the  
19                   portion of the web site subject to the access attempt.
- 1           2.     The computer program product of claim 1 further comprising  
2 computer readable program code means for carrying out the determination of the  
3 access role associated with a user identity for a security domain at user logon time.
- 1           3.     The computer program product of claim 1 in which the set of access  
2 roles comprises registered customer and administrator roles.

1           4.     The computer program product of claim 1, further comprising  
2 computer readable program code means to define the set of organizations as a tree  
3 structure, in which the computer readable program code means for associating a user  
4 identity with one of a set of access roles further comprises computer readable  
5 program code means for associating the user identity with the access role for a  
6 selected one of the set of organizations; and

7           computer readable program code means for defining the security domain to  
8           include the selected organization and those organizations in the set that  
9           are descendants of the selected organization.

1           5.     The computer program product of claim 2, further comprising:  
2 computer readable program code means to define the set of organizations as a  
3 tree structure, in which the computer readable program code means for  
4 associating a user identity with one of a set of access roles further  
5 comprises computer readable program code means for associating the  
6 user identity with the access role for a selected one of the set of  
7 organizations; and  
8 computer readable program code means for defining the security domain to  
9 include the selected organization and those organizations in the set that  
10 are descendants of the selected organization.

1           6.     The computer program product of claim 3, further comprising:  
2 computer readable program code means to define the set of organizations as a  
3 tree structure, in which the computer readable program code means for  
4 associating a user identity with one of a set of access roles further  
5 comprises computer readable program code means for associating the  
6 user identity with the access role for a selected one of the set of  
7 organizations; and

8           and further comprising computer readable program code means for defining  
9           the security domain to include the selected organization and those  
10          organizations in the set that are descendants of the selected  
11          organization.

1           7.     The computer program product of claim 4 in which the computer  
2     readable program code means for associating a user identity with one of a set of  
3     accessible roles comprises computer readable program code means for maintaining  
4     and providing look up functionality for a table comprising rows comprising data  
5     representing user identity, organization, access role associations.

1           8.     The computer program product of claim 1, further comprising  
2     computer readable program code means for providing user identities with associated  
3     access roles at user registration to the web site.

1           9.     A system for implementing electronic commerce systems, each  
2 electronic commerce system comprising a web site being accessible by one or more  
3 users and comprising a set of on-line stores and a set of organizations, each of the  
4 said on-line stores being associated with one of the set of organizations, the system  
5 comprising:

6               means for representing the users, each user being associated with a unique  
7               identity in the system;

8               means for associating a user identity with one of a set of access roles for a  
9               security domain, the access role defining access privileges for the user  
10              corresponding to the user identity, the security domain comprising a  
11              subset of the set of organizations and the on-line stores associated with  
12              the organizations in the subset; and

13              means for granting or denying access to a user attempting to access a portion  
14              of the web site by determining the user identity for the user and  
15              determining the access role associated with the user identity for the  
16              security domain corresponding to the portion of the web site subject to  
17              the access attempt.

1           10.    The system of claim 9 further comprising means for carrying out the  
2 determination of the access role associated with a user identity for a security domain  
3 at user logon time.

1           11.    The system of claim 9 in which the set of access roles comprises  
2 registered customer and administrator roles.

1           12.    The system of claim 9, further comprising  
2               means to define the set of organizations as a tree structure, in which the means  
3               for associating a user identity with one of a set of access roles further  
4               comprises means for associating the user identity with the access role  
5               for a selected one of the set of organizations; and

6 means for defining the security domain to include the selected organization  
7 and those organizations in the set that are descendants of the selected  
8 organization.

1 13. The system of claim 10, further comprising:  
2 means to define the set of organizations as a tree structure, in which the means  
3 for associating a user identity with one of a set of access roles further  
4 comprises means for associating the user identity with the access role  
5 for a selected one of the set of organizations; and  
6 means for defining the security domain to include the selected organization  
7 and those organizations in the set that are descendants of the selected  
8 organization.

1 14. The system of claim 11, further comprising:  
2 means to define the set of organizations as a tree structure,  
3 in which the means for associating a user identity with one of a set of access  
4 roles further comprises means for associating the user identity with the  
5 access role for a selected one of the set of organizations; and  
6 means for defining the security domain to include the selected organization  
7 and those organizations in the set that are descendants of the selected  
8 organization.

1 15. The system of claim 12 in which the means for associating a user  
2 identity with one of a set of accessible roles comprises means for maintaining and  
3 providing look up functionality for a table comprising rows comprising data  
4 representing user identity, organization, access role associations.

1 16. The system of claim 9, further comprising means for providing user  
2 identities with associated access roles at user registration to the web site.

1           17. A method for providing user access to a portion of a web site  
2 implemented by an electronic commerce system, the web site being accessible by one  
3 or more users and comprising a set of on-line stores and a set of organizations, each  
4 of the said on-line stores being associated with one of the set of organizations, the  
5 method comprising the steps of:

6           associating each user with a unique identity in the system;

7           associating a user identity with one of a set of access roles for a security  
8 domain, the access role defining access privileges for the user  
9 corresponding to the user identity, the security domain comprising a  
10 subset of the set of organizations and the on-line stores associated with  
11 the organizations in the subset; and

12          granting or denying access to a user attempting to access a portion of the web  
13 site by determining the user identity for the user and determining the  
14 access role associated with the user identity for the security domain  
15 corresponding to the portion of the web site subject to the access  
16 attempt.

1           18. The method of claim 17 in which the step of carrying out the  
2 determination of the access role associated with a user identity for a security domain  
3 occurs at user logon time.

1           19. The method of claim 17 in which the set of access roles comprises  
2 registered customer and administrator roles.

1           20. The method of claim 17 in which the set of organizations is a tree  
2 structure, the step of associating a user identity with one of a set of access roles  
3 further comprises the step of associating the user identity with the access role for a  
4 selected one of the set of organizations,

5           the security domain includes the selected organization and those organizations  
6           in the set that are descendants of the selected organization, and

7           the step of granting or denying access by determining the access role  
8           associated with the user identity for the security domain comprises  
9           determining the access role for the user identity by traversing the tree  
10          structure of organizations commencing at the selected organization and  
11          including the ancestor organizations to the selected organization.

1           21.    The method of claim 18 in which  
2           the set of organizations is a tree structure,  
3           the step of associating a user identity with one of a set of access roles further  
4           comprises the step of associating the user identity with the access role  
5           for a selected one of the set of organizations, and  
6           the security domain includes the selected organization and those organizations  
7           in the set that are descendants of the selected organization.

1           22.    The method of claim 19 in which  
2           the set of organizations is a tree structure,  
3           the step of associating a user identity with one of a set of access roles further  
4           comprises the step of associating the user identity with the access role  
5           for a selected one of the set of organizations, and  
6           the security domain includes the selected organization and those organizations  
7           in the set that are descendants of the selected organization.

1           23.    The method of claim 20 in which the step of associating a user identity  
2           with one of a set of accessible roles comprises entering data in a table comprising  
3           rows comprising data representing user identity, organization, access role  
4           associations.

5           24.    The method of claim 17 in which the step of providing user identities  
          with associated access roles occurs at the time of user registration to the web site.